Program of the 4th DAAD Summer School CTDS 2012

September 6th to 8th 2012, Hotel Elmouradi Palace, Sousse – Tunisia

Time	Thu 06.09.12	Fri 07.09.12	Sat 08.09.12
8:00-8:45	Registration		
8:45-9:00	Opening Session		
9:00-9:30	**Session 1:** Introduction to Cloud Computing **Dr. Marcel Kunze**	**Session 5:** Usable Security for the Cloud **Prof. Mathew Smith**	**Session 8:** Security of Cloud Storage **Sven Vowé**
9:30-10:00			
10:00-10:30			
10:30-11:00	Break	Break	Break
11:00-11:30	**Session 2:** Introduction to Cloud Computing **Dr. Marcel Kunze**	**Session 6:** Homomorphic Cryptography for Cloud Computing **Henning Perl**	**Session 9:** Cloud Computing from an Industry Perspective **Rana Khalil**
11:30-12:00			
12:00-12:30		**Session 7:** Overview of the FlexCloud project **Yvonne Thoss** **Anja Strunk**	
12:30-13:00	Lunch		Lunch
13:00-13:30		Lunch	
13:30-14:00	**Session 3:** Elastic-R. A SaaS for Scientific Computing **Karim Chine**		
14:00-14:30			
14:30-15:00			
15:00-15:30	Break	Social Program: Excursion & Banquet	
15:30-16:00	**Session 4:** Tutorial: Develop Cloud Applications with Google App Engine **Benjamin Schmeling**		
16:00-16:30			
16:30-17:00			

The session details can be found on the next pages.

Sessions 1 and 2:
Introduction to Cloud Computing

Dr. Marcel Kunze

Abstract: Building on compute, storage, network, and business virtualization Cloud Computing provides scalable, network-centric, abstracted IT infrastructure, platforms, and applications as on-demand services that are billed by consumption. In its fifth year of existence it is evident that Cloud Computing leads to a paradigm shift in IT: It transforms fixed cost into variable cost, thus improving cost effectiveness. It increases business agility, thus shortening time to market. And it creates opportunities for new applications and business models that may not be feasible with classical IT solutions. This lecture introduces fundamentals of Cloud Computing, providing an overview of state-of-the-art in research and practice.

Biography: Dr. Marcel Kunze performs systems research in the area of dynamic and scalable web based services at the Karlsruhe Institute for Technology (KIT). He is committed to R&D in the field of service oriented architectures, virtualization techniques and system development. His working groups are engaged in many national and international research projects such as Software-Cluster, trusted cloud initiative, and the Open Cirrus cloud computing testbed under the sponsorship of HP, Intel and Yahoo! He is a member of the editorial board of the GSTF International Journal on Computing and the new Springer Journal of Cloud Computing. He is one of the authors of the well-known Springer cloud computing book. Dr. Kunze received a PhD in Physics at Karlsruhe University in 1990 and finished a habilitation thesis on artificial neural systems at Bochum University in 1996. Since then he joined SLAC / Stanford University to investigate and further develop the Grid Computing paradigm for distributed processing of particle physics data. As an associate professor he was teaching particle physics, distributed systems and software design. In 2002 Dr. Kunze joined Research Centre Karlsruhe as a department leader for "Grid Computing and e-Science" to work on the establishment of the LHC Computing Grid and the German D-Grid initiative. With the transition to KIT, as a leading scientist Dr. Kunze is heading a cloud computing research group at the Steinbuch Centre for Computing (SCC) and a cloud computing lab at the Engineering and Mathematics Computing Lab (EMCL).

Sessions 3:
What the Cloud can do for Data Science

Karim Chine

Abstract: Cloud computing is the answer to the explosion of data and while the cloud already provides infinite scalability for storage, data analysis in the cloud is still making its first steps. Elastic-R proposes to build on top of Infrastructure-as-a-service-style clouds, such as EC2, a ubiquitous collaborative virtual environment for participatory data analysis. The Elastic-R frameworks leverage the programmability of EC2 and propose new abstractions for building robust Analytics-as-a-Service capabilities in the cloud. Thanks to those frameworks, rapid analytical applications/services prototyping and publication is dramatically simplified and becomes accessible to the vast majority of data scientists. Finally, thanks to the ""elasticR" package, the cloud and its manipulation become accessible from the R command line as well as real-time collaboration and the sharing of all the produced artifacts. The presentation will give an overview of Elastic-R and will demonstrate its main capabilities.

References

[1] Elastic-R Platform, http://www.elastic-r.net.

[2] Karim Chine (2010). Open science in the cloud: towards a universal platform for scientific and statistical computing. In: Furht B, Escalante A (eds) Handbook of cloud computing, Springer, USA, pp 453–474. ISBN 978-1-4419-6524-0.

[3] Karim Chine (2010). Learning math and statistics on the cloud, towards an EC2-based Google Docs-like portal for teaching / learning collaboratively with R and Scilab, icalt, pp.752-753, 2010 10th IEEE International Conference on Advanced Learning Technologies.

Biography: Karim Chine is a software architect, an entrepreneur and a European commission's cloud computing and research infrastructures' expert. After graduating from the French Ecole Polytechnique and Telecom ParisTech, he occupied various positions within Industry and Academia. Karim was a stuff member respectively at Schlumberger, IBM, EBI and Imperial College London. He is the founder of cloud era, a UK-based start-up specializing in scientific software-as-a-service. Karim is the author and designer of Elastic-R, a pioneering Virtual Research Environment for scientific and statistical computing, reproducible research and collaboration in the cloud.

Session 4:
Develop Cloud Applications with Google App Engine,

Benjamin Schmeling

Abstract: In this tutorial the Google App Engine (GAE) is introduced and it is shown how to develop and deploy web applications for this popular Platform as a Service (PaaS) offering. The application is developed with the new Eclipse IDE Juno (4.2) including the GAE plugins. The web application is based on state-of-the-art Java web standards and uses the Java Persistency API to access Google's Datastore.

Google offers a variety of platform services such as Authentication, Email, Image Manipulation and many more. It is shown how these services can be consumed and integrated into the web application. The application is demonstrated on a local server and then deployed remotely on the App Engine where it is directly available over the Internet. Finally, an overview of the administration options supported by GAE is given.

Biography: Benjamin Schmeling works at SAP Research in Darmstadt on the german research project Software Cluster, which investigates next generation cloud-based business software platforms. After his studies at Technical University of Darmstadt in 2005 he started to work as a software engineer and consultant developing model-driven software solutions. He is an committer for the Fornax project where he is responsible for the JPA and JSF cartridges for Open Architecture Ware. Since 2009 he pursues his PhD in the Software Technology Group at Technical University of Darmstadt. His current research interests lie in service-oriented architectures, especially web service composition, the modularization of non-functional concerns and cloud computing.

Session 5:
Usable Security for the Cloud

Prof. Matthew Smith

Abstract: Useable security and privacy is a field of research gaining ever more momentum as ever more online-activities are done by non-IT experts and the number of actors and the complexity of online systems is fast outpacing our capability of creating security mechanisms which work well for the average user. New computing paradigms such as Cloud, Web 2.0 and mobile computing are driving these changes and are creating new challenges for security and privacy. Due to these technologies we are seeing a shift from users who merely consume content to an active and thriving community that autonomously creates and interlinks content. Since the sharing of data is no longer the sole domain of system administrators, average users now bear a large part of the responsibility of securing their data and their privacy. Conflicting interests of service providers further add to these problems. The combination of Cloud, Web 2.0 and mobile computing is fast making the “Cloud” a central hub of our digital lives, containing a vast amount of privacy relevant information. Bad usability of security and privacy mechanisms often leads to a complete failure or bypassing of these systems. In this talk it will be argued that it is necessary to integrate security technology into the existing usage pattern in a non-disruptive way. The concept of security and privacy as a service (S&PaaS) will be introduced. In order to integrate the security and privacy mechanisms into existing services the mental user model must be considered in order to develop clear and comprehensible systems. Another important aspect of S&PaaS can be found in an international context. While web and cloud services become ever more location independent, security and privacy requirements are often specific to a country, organization or person. S&PaaS makes it possible for custom security and privacy offers to be integrated as services in existing cloud and web applications and thereby to fulfill the diverse needs and usage wishes. These concepts will be illustrated using examples from security and privacy of online social networks and Cloud services such as Dropbox. The talk will then change gear and show how the application of the internet and cloud services brought on by the proliferation of dedicated smart phone apps, is changing the way we use the both the Internet and Cloud services and the effect on security and privacy. In particular it will be shown how the application has pushed the burden of security and privacy onto the shoulders of App developers and how security needs to become more usable not only for end users but also for developers.

Biography: Prof. Smith is a Professor of Computer Science at the Leibniz Universität Hannover, Germany where he leads the Distributed Computing & Security Group. He completed his studies of Computer Science & Electrical Engineering at the University of Siegen, Germany with distinction. Subsequently he was a full time researcher at the Philipps Universität Marburg, Germany where he completed his PhD in 2008, also with distinction. In 2009 he was awarded the PhD Prize for outstanding innovation by the Gesellschaft zur Förderung des Forschungstransfers (GFFT e.V.). His current research is focused on the usability aspects of security and privacy mechanisms with a wide range of application areas. These areas include Cloud Computing, e-Research Infrastructures, Social Networking and Mobile Computing. He is a member of IEEE and the ACM SIGSAC.

Session 6:
Homomorphic Cryptography for Cloud Computing

Henning Perl

Abstract: Homomorphic cryptography has long been the Holy Grail of cryptography, until a first encryption scheme was discovered by Craig Gentry in 2009. The potential power in this new kind of schemes lies in the fact that arithmetic operations, i.e. addition and multiplication, are possible (and meaningful) on the encrypted cipher text. More specifically, the encryption and decryption functions are homomorphisms from the plain text space to the cipher text space. Although this is with no doubt a great breakthrough, there are still many steps to take and open problems to solve to go from a homomorphic encryption scheme to use cases like confidential computation in the cloud.

This talk will start with a short overview of Gentry's original scheme as well as the somewhat-homomorphic schemes that led up to it. Then, an easy to understand somewhat-homomorphic scheme will be presented in detail. This will be applied in the second part of the talk when looking at the construction of a CPU that works completely in the encrypted domain. This means that everything, including program data and code, is encrypted as well as that the memory access is oblivious. In the last part of the talk a close look will be taken at real-world applications of these new technologies. A naive application of homomorphic encryption to guaranteeing confidentiality has a high performance penalty. In order to tap into the real power of homomorphic encryption, a move towards hybrid systems is needed, where through a careful analysis of a given use case only those parts of an algorithm are run in the protected cipher space that need confidentiality. By running only a small part of the algorithm using homomorphic encryption, balances can be found where the whole algorithm performs only marginally worse than the unencrypted counterpart.

Biography: Henning Perl received his master’s degree in computer science in December 2011 from the Leibniz University Hanover, Germany and joined the university's Distributed Computing & Security Group in January 2012 as a doctorate student. While he was still a graduate student he developed the first open-source homomorphic cryptography library. His research interests include homomorphic cryptography and its application in Cloud Computing and he is one of the lead developers of hCrypt.com.

Session 7: Overview of the FlexCloud project

Yvonne Thoss & Anja Strunk

Abstract 1: Virtualization and broadband Internet connections enabled existing technologies to form up under the nebulous term cloud. Cloud computing promises near infinite scalability and cost reduction by pay per use agreements. However for data outsourced to existing cloud solutions - which can be considered synonymous with unknown locations and potentially hostile environments - the security protection objectives cannot be guaranteed. We present an approach that enables users to benefit from cloud computing and retain data sovereignty.

Biography: Anja Strunk is working at the Technical University of Dresden, where she studied computer science and graduated in 2006. Subsequently to her final degree, she started to work as full time research assistant at the Technical University of Dresden and joined the chair of computer networks. Her research interest was the Internet of services, especially Quality of Service (QoS) of business processes using parts of the Internet of Services. Anja Strunk received her PhD in 2010 and changed over to cloud computing, where she is investigating efficiency and security of cloud computing.

Abstract 2: This presentation is going to introduce the topic of the management and optimization of the cloud service usage for end users without expert knowledge. The first part is about the cloud service lifecycle and introduces different cloud user roles including their activities. After comparing several cloud management systems it presents the need and first results for supporting end users without expert knowledge beyond that. This subject is important for the "personal secure cloud" or "Π-Cloud" that is defined within the FlexCloud project. The Π-Cloud is a hybrid cloud that covers all resources, services and data under complete control of a user. The presentation talks about the early research results regarding my doctoral thesis, in the hope to obtain feedback about the importance of this research subject.

Biography: Yvonne Thoss
WORK, since April 2011:
Position: Research assistant & Ph.D. student at Technische Universität Dresden, Germany
Faculty of Computer Science Institute of Systems Architecture, Chair of Computer Networks
Project: FlexCloud - Flexible Service Architectures for Cloud Computing
Website for further details: http://flexcloud.eu/?lang=en

STUDIES:
University: Technische Universität Dresden, Germany
Program: Media Computer Science Degree:
German Diplom (equivalent of master)
Finished: March 2011

Session 8:
Cloud Storage Security

Sven Vowé

Abstract: Recently, a multitude of Cloud Storage Services have appeared on the market, offering data storage to protect users against irrevocable data loss or to provide a cost-saving data sink for arbitrary online services. Basic cloud storage services (such as Amazon S3) provide a rudimentary API for data storage/retrieval and aim to be used by third-party software. Advanced cloud storage services target end-users by providing user-friendly and easily accessible features to back up private data. These services have evolved to encompass data synchronization across multiple devices, sharing with other users and publication. Since security requirements for the protection of sensitive data are already very high, the added software complexity introduces new attack surfaces. Most service providers have implemented security measures, but many fall short compared to the needs of corporations and private individuals alike.

The talk will provide an overview of the key properties of Cloud Storage Services and their capabilities. Subsequently, mandatory and optional security requirements are presented, mainly concerning the fields of user handling, data transport, encryption, sharing and deduplication technology. Several Cloud Storage Services (such as Dropbox, Mozy, Ubuntu One) have been thoroughly tested by Fraunhofer SIT in 2011 – the key results will be summarized within the talk. The talk closes with a short presentation of simple but effective impersonation attacks found and published by SIT in 2012.

Biography: Sven Vowé, Dipl. Inform., 2008 diploma in Computer Science from University of Technology Darmstadt, Germany with emphasis on IT-Security and Cryptography. He joined the Fraunhofer Institute for Security Information Technology (SIT) scientific staff in the same year and has been working in the department 'Transactional and Document Security', performing security analysis and concepts for web applications, email-gateways, data encryption and smart card technology.

As part time personnel of Security Test-Lab (STL), he conducted several web application penetration tests for external customers. In late 2010, he joined the newly formed department 'Cloud, Identity and Privacy' (CIP), where his core activities encompass vulnerability analysis, security concepts and practical security in the field of Cloud Computing, and particularly Cloud Storage Systems.

Session 9:
Cloud computing from an industrial perspective

Rana Khalil

Abstract: EMC is one the leading companies worldwide in Cloud Computing. This talk will give an overview of the company activities around this topic and also motivates why EMC believes that Cloud Computing is the next big thing. In addition, the talk will show the benefits of cloud computing that were gained by EMC customer in real projects. The talk will also address the different cloud deployment models and also the differences between the way EMC looks and works on Cloud Computing compared to other cloud service providers.

Biography: Rana Ahmed Khalil, got her B.Sc in Digital Media Engineering and Technology, the German University in Cairo, June 2010. From August 2010 till April 2012, she worked at Mobinil – a telecommunication operator within its ERP (Enterprise Resource Planning) department. In April 2012, Rana joined EMC, working as a project Manager, after attending GSAP, a 5 weeks EMC international program in Boston, USA.
Within her years as student she have trained in several multination companies such as IBM, Orange, Vodafone, and was also a trainee at ULM University in Germany.